JASON M. WUCETICH (STATE BAR NO. 222113)
jason@wukolaw.com
DIMITRIOS V. KOROVILAS (STATE BAR NO. 247230)
dimitri@wukolaw.com
WUCETICH & KOROVILAS LLP
222 N. Pacific Coast Hwy., Suite 2000
El Segundo, CA 90245
Telephone: (310) 335-2001
Facsimile: (310) 364-5201

Attorneys for Plaintiff
ANTONIO HOOD, individually and on behalf of all others similarly situated

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

ANTONIO HOOD, individually and on behalf of all others similarly situated, Plaintiff, v. DRIVE SALLY, LLC; and DOES 1-10, Defendants.	CASE NO. CLASS ACTION COMPLAINT FOR: (1) NEGLIGENCE (2) NEGLIGENCE PER SE (3) DECLARATORY JUDGMENT (4) VIOLATION OF THE CAL. CONSUMER PRIVACY ACT, CAL. CIV. CODE § 1798.150 (5) VIOLATION OF THE CAL. CUSTOMER RECORDS ACT, CAL. CIV. CODE § 1798.84 (6) VIOLATION OF THE CAL. UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200 (7) VIOLATION OF THE RIGHT TO PRIVACY, CAL. CONST. ART. 1, § 1 (8) BREAH OF IMPLIED CONTRACT (9) BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING DEMAND FOR JURY TRIAL

SUMMARY OF THE CASE

1. This putative class action arises from Drive Sally, LLC's (hereinafter "DEFENDANT") negligent failure to implement and maintain reasonable cybersecurity procedures that resulted in a data breach of its systems that was discovered on or around May 1, 2024. In connection with the Data Breach, DEFENDANT failed to properly secure and safeguard Plaintiff's and Class Members' protected personally identifiable information, including without limitation, full names, driver's license numbers and dates of birth (these types of information, *inter alia*, being thereafter referred to, collectively, as "personal identifiable information" or "PII").[1] While DEFENDANT claims to have discovered the breach in May 2024, they did not start informing victims of the Data Breach for over a month and their notice letter was vague of any specific details regarding when the breach occurred. Plaintiff brings this class action complaint to redress injuries related to the Data Breach, on behalf of himself and a nationwide class and a California subclass of similarly situated persons. Plaintiff asserts claims on behalf of a nationwide class for negligence, negligence per se, declaratory judgment, common law invasion of privacy, breach of implied contract and breach of implied covenant of good faith and fair dealing. Plaintiff also brings claims on behalf of a California subclass for violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, the California Customer Records Act, Cal. Civ. Code § 1798.80 *et seq.*, violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*, and for invasion of privacy based on the California Constitution, Art. 1, § 1. Plaintiff seeks, among other things,

[1] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

compensatory damages, punitive and exemplary damages, injunctive relief, attorneys' fees, and costs of suit. Plaintiff further intends to amend this complaint to seek statutory damages on behalf of the California subclass upon expiration of the 30-day cure period pursuant to Cal. Civ. Code § 1798.150(b).

PARTIES

2. Plaintiff Antonio Hood is a citizen and resident of the State of California, residing in Los Angeles, California, whose personal identifying information was part of the May 2024 data breach that is the subject of this action.

3. On information and belief, Defendant Drive Sally, LLC is a corporation organized under the laws of Delaware with its principal place of business located in Long Island City, New York. Drive Sally, LLC has previously maintained offices within Southern California and within the Central District, including in El Segundo, California.

4. Plaintiff bring this action on behalf of himself, on behalf of the general public as a Private Attorney General pursuant to California Code of Civil Procedure § 1021.5 and on behalf of a class and subclass of similarly situated persons pursuant Federal Rule of Civil Procedure 23.

JURISDICTION & VENUE

5. This Court has general personal jurisdiction over DEFENDANT because, at all relevant times, the company had systematic and continuous contacts with the State of California. DEFENDANT does business in California and has previously had offices within the Central District. DEFENDANT regularly contracts with a multitude of businesses, organizations and consumers in California to provide car rental related services. DEFENDANT does in fact actually provide such continuous and ongoing car rental related services to such customers in California and has employees in California.

6. Furthermore, this Court has specific personal jurisdiction over DEFENDANT because the claims in this action stem from its specific contacts with

the State of California — namely, DEFENDANT'S provision of car rental related services to a multitude of clients in California, DEFENDANT'S collection, maintenance, and processing of the personal data of Californians in connection with such services, including but not limited to DEFENDANT'S employees, DEFENDANT'S failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent cybersecurity attack and security breach of such data in May 2024.

7. This Court has diversity subject matter jurisdiction under 28 U.S.C. § 1332(d) in that the mater in controversy exceeds the sum or value of $5,000,000, exclusive of interests and costs, and is a class action in which members of the class defined herein include citizens of a State different from the DEFENDANT.

8. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court pursuant to 28 U.S.C. § 1367.

9. Venue is proper in the Central District of California under 28 U.S.C. § 1391 (b)(1)-(2) and (c)(2) because a substantial part of the events or omissions giving rise to the claims alleged herein occurred within this judicial district, specifically DEFENDANT'S provision of car rental related services in California and within Los Angeles County, DEFENDANT'S collection, maintenance, and processing of the personal data of Californians in connection with such services, DEFENDANT'S failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent security breach of such data in May 2024 that resulted from DEFENDANT'S failure. In addition, Plaintiff is informed and believes and thereon alleges that members of the class and subclass defined below reside in the Central District, and DEFENDANT has and/or previously had offices within the Central District, including during the statutory period of this lawsuit.

FACTUAL BACKGROUND

10. Drive Sally, LLC is a company that provides rental cars and related

services primarily to Uber and Lyft drivers.

11. Plaintiff rented a car from DEFENDANT in El Segundo, California for the purpose of driving for Uber and Lyft.

12. In connection with its rental car business, DEFENDANT collects, stores, and processes sensitive personal data for tens of thousands of individuals, including but not limited to its clients and employees. In doing so, DEFENDANT retains sensitive information including, but not limited to, financial information, addresses, driver's license numbers, dates of birth, and social security numbers, among other things.

13. As a company doing business in California and having employees and clients in California, DEFENDANT is legally required to protect personal information from unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction.

14. DEFENDANT knew that they were a prime target for hackers given the significant amount of sensitive personal information processed through its computer data and storage systems. DEFENDANT'S knowledge is underscored by the massive number of data breaches that have occurred in recent years.

15. Despite knowing the prevalence of data breaches, DEFENDANT failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to its highly sensitive systems and databases. DEFENDANT has the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized breaches. DEFENDANT failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures as described herein to ensure vulnerabilities were avoided or remedied and that Plaintiff's and Class Members' data were protected.

16. Specifically, on or around May 1, 2024, DEFENDANT discovered a significant cybersecurity breach. DEFENDANT'S subsequent investigation

revealed that a number of sensitive information may have been taken from DEFENDANT'S files and information technology systems by unauthorized third parties.

17. On information and belief, the personal information DEFENDANT collects and which was impacted by the cybersecurity attack includes individuals' name, driver's license number and date of birth, among other personal, sensitive and confidential information.

18. On or around June 5, 2024, DEFENDANT mailed and/or emailed data breach notices to impacted parties. According to notice to impacted individuals, the breach resulted in individuals' name, driver's license number and date of birth being compromised and exfiltrated by unauthorized actors. Plaintiff received a copy of the June 5, 2024 data breach notice via electronic mail confirming that his personal identifying information was part of the data breach.

19. Upon information and belief, the hackers responsible for the Data Breach stole the personal information many of DEFENDANT'S clients and employees, including Plaintiff's. Because of the nature of the breach and of the personal information stored or processed by DEFENDANT, Plaintiff is informed and believes that all categories of personal information were further subject to unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction. Plaintiff is informed and believes that criminals would have no purpose for hacking DEFENDANT other than to exfiltrate or steal, or destroy, use, or modify as part of their ransom attempts, the coveted personal information stored or processed by DEFENDANT.

20. The personal information exposed by DEFENDANT as a result of its inadequate data security is highly valuable on the black market to phishers, hackers, identity thieves, and cybercriminals. Stolen personal information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web

due to this encryption, which allows users and criminals to conceal identities and online activity.

21. When malicious actors infiltrate companies and copy and exfiltrate the personal information that those companies store, or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.

22. The information compromised in this unauthorized cybersecurity attack involves sensitive personal identifying information, which is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. Whereas here, the information compromised is difficult and highly problematic to change—particularly social security numbers.

23. Once personal information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional personal information being harvested from the victim, as well as personal information from family, friends, and colleagues of the original victim.

24. Unauthorized data breaches, such as these, facilitate identity theft as hackers obtain consumers' personal information and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' personal information to others who do the same.

25. The high value of PII to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[2]

[2] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the- dark-web-

Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[3] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[4]

26. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

27. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

28. Identity thieves can use PII, such as that of Plaintiffs and Class Members which DEFENDANT failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types

---

how-much-it-costs/ (last accessed July 28, 2021).

[3] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed November 5, 2021).

[4] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed January 21, 2022).

of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

29. The ramifications of DEFENDANT'S failure to keep secure Plaintiff's and Class Members' PII are long lasting and severe. Once PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, Plaintiff's and Class Members' PII was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

30. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[5]

31. When cyber criminals access financial information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Plaintiffs and Class Members.

32. And data breaches are preventable.[6] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data

[5] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed January 21, 2022).

[6] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson,

breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[7] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[8]

33. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.[9]

34. Federal and state governments have established security standards and issued recommendations to minimize unauthorized data disclosures and the resulting harm to individuals and financial institutions. Indeed, the Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices.

35. According to the FTC, the need for data security should be factored into all business decision-making.[10] In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[11] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed, encrypt information stored on

---

ed., 2012)

[7] *Id.* at 17.

[8] *Id.* at 28.

[9] *Id.*

[10] *See* Federal Trade Commission, Start with Security (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited February 3, 2023).

[11] *See* Federal Trade Commission, Protecting Personal Information: A Guide for Business (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited February 3, 2023).

computer networks, understand their network's vulnerabilities, and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of the breach.

36. Also, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[12]

37. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect personal information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45.

38. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

39. The FBI created a technical guidance document for Chief Information Officers and Chief Information Security Officers that compiles already existing federal government and private industry best practices and mitigation strategies to prevent and respond to ransomware attacks. The document is titled *How to Protect Your Networks from Ransomware* and states that on average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. Yet, there are very effective prevention and response actions that can significantly mitigate the risks.[13]

[12] *See id.*

[13] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last viewed February 3, 2023).

Preventative measure include:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[14]

40. DEFENDANT could have prevented the cybersecurity attack by properly utilizing best practices as advised by the federal government, as described in the preceding paragraphs, but failed to do so.

41. DEFENDANT'S failure to safeguard against a cybersecurity attack is exacerbated by the repeated warnings and alerts from public and private institutions, including the federal government, directed to protecting and securing sensitive data. Experts studying cybersecurity routinely identify companies such as DEFENDANT that collect, process, and store massive amounts of data on cloud-based systems as being particularly vulnerable to cyberattacks because of the value of the personal information that they collect and maintain. Accordingly, DEFENDANT knew or should have known that they were a prime target for hackers.

42. According to the 2021 Thales Global Cloud Security Study, more than 40% of organizations experienced a cloud-based data breach in the previous 12 months. Yet, despite these incidents, the study found that nearly 83% of cloud-based businesses still fail to encrypt half of the sensitive data they store in the cloud.[15]

43. Upon information and belief, DEFENDANT did not encrypt Plaintiff's and Class Members' personal information involved in the data breach.

44. Despite knowing the prevalence of data breaches, DEFENDANT failed to prioritize cybersecurity by adopting reasonable security measures to prevent and detect unauthorized access to its highly sensitive systems and

[14] *Id.*

[15] Maria Henriquez, *40% of organizations have suffered a cloud-based data breach,* Security, Oct. 29, 2021, https://www.securitymagazine.com/articles/96412-40-of-organizations-have-suffered-a-cloud-based-datq-breach (last visited February 3, 2023).

databases. DEFENDANT has the resources to prevent an attack, but neglected to adequately invest in cybersecurity, despite the growing number of well-publicized breaches. DEFENDANT failed to fully implement each and all of the above-described data security best practices. DEFENDANT further failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures to ensure vulnerabilities were avoided or remedied and that Plaintiff's and Class Members' data were protected.

45. As detailed above, DEFENDANT is a large, sophisticated rental car company with the resources to deploy robust cybersecurity protocols. They knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff and Class Members. Its failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent.

46. DEFENDANT disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

Plaintiff's Facts

47. DEFENDANT received highly sensitive PII from Plaintiff when he rented a car from DEFENDANT. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

48. At all times herein relevant, Plaintiff is and was a member of the nationwide class and the California subclass alleged herein.

49. Plaintiff's PII was exposed in the Data Breach because DEFENDANT stored and/or controlled Plaintiff's PII. Plaintiff's PII was within the possession and control of DEFENDANT at the time of the Data Breach.

50. Plaintiff received an electronic mail message from Defendant, dated June 5, 2024, stating that his name, driver's license number and date of birth was in the possession, custody and/or control of DEFENDANT and was involved in the Data Breach (the "Notice").

51. As a result, Plaintiff spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring his accounts and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

52. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to DEFENDANT, which was compromised in and as a result of the Data Breach.

53. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his PII and/or financial information.

54. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

55. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in DEFENDANT'S possession, is protected and safeguarded from future breaches.

56. Plaintiff and Class Members have spent and will continue to spend time and effort monitoring his accounts to protect themselves from identity theft. Plaintiff and Class Members remain concerned for their personal security and the uncertainty of what personal information was exposed to hackers and/or posted to the dark web.

57. As a direct and foreseeable result of DEFENDANT'S negligent failure to implement and maintain reasonable data security procedures and practices and the resultant breach of its systems, Plaintiff and all Class Members, have suffered harm in that their sensitive personal information has been exposed to cybercriminals and they have an increased stress, risk, and fear of identity theft and fraud. This is not just a generalized anxiety of possible identify theft, privacy, or fraud concerns, but a concrete stress and risk of harm resulting from an actual breach and accompanied by actual instances of reported problems suspected to stem from the breach.

58. Plaintiff and Class Members are especially concerned about the misappropriation of their Social Security numbers. Social security numbers are among the most sensitive kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's social security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls

> from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[16]

59. Furthermore, Plaintiff and Class Members are well aware that their sensitive personal information, including social security numbers and potentially banking information, risks being available to other cybercriminals on the dark web. Accordingly, all Plaintiff and Class Members have suffered harm in the form of increased stress, fear, and risk of identity theft and fraud resulting from the data breach. Additionally, Plaintiff and Class Members have incurred, and/or will incur, out-of-pocket expenses related to credit monitoring and identify theft prevention to address these concerns.

CLASS ACTION ALLEGATIONS

60. Plaintiff bring this action on behalf of himself and all other similarly situated persons pursuant to Federal Rule of Civil Procedure 23, including Rule 23(b)(1)-(3) and (c)(4). Plaintiff seek to represent the following class and subclass:

> **Nationwide Class**. All persons in the United States whose personal information was compromised in or as a result of DEFENDANT'S data breach discovered by DEFENDANT on or around May 1, 2024.

> **California Subclass.** All persons residing in California whose personal information was compromised in or as a result of DEFENDANT'S data breach discovered by DEFENDANT on or around May 1, 2024.

Excluded from the class are the following individuals and/or entities: DEFENDANT and their parents, subsidiaries, affiliates, officers, directors, or employees, and any entity in which DEFENDANT has a controlling interest; all individuals who make a timely request to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this

[16] *Identify Theft and Your Social Security Number*, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited February 3, 2023).

litigation, as well as their immediate family members.

61. Plaintiff reserves the right to amend or modify the class definitions with greater particularity or further division into subclasses or limitation to particular issues.

62. This action has been brought and may be maintained as a class action under Rule 23 because there is a well-defined community of interest in the litigation and the proposed classes are ascertainable, as described further below:

a. Numerosity: The potential members of the class as defined are so numerous that joinder of all members of the class is impracticable. While the precise number of Class Members at issue has not been determined, Plaintiff believes the cybersecurity breach affected tens of thousands of individuals nationwide and at least many thousands within California.

b. Commonality: There are questions of law and fact common to Plaintiffs and the class that predominate over any questions affecting only the individual members of the class. The common questions of law and fact include, but are not limited to, the following:

i. Whether DEFENDANT owed a duty to Plaintiff and Class Members to exercise due care in collecting, storing, processing, and safeguarding their personal information;

ii. Whether DEFENDANT breached those duties;

iii. Whether DEFENDANT implemented and maintained reasonable security procedures and practices appropriate to the nature of the personal information of Class Members;

iv. Whether DEFENDANT acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class Members' personal information;

v. Whether DEFENDANT knew or should have known that they did not employ reasonable measures to keep Plaintiff's and Class Members' personal information secure and prevent loss or misuse of that personal information;

vi. Whether DEFENDANT adequately addressed and fixed the vulnerabilities which permitted the data breach to occur;

vii. Whether DEFENDANT caused Plaintiff and Class Members damages;

viii. Whether the damages DEFENDANT caused to Plaintiff and Class Members includes the increased risk and fear of identity theft and fraud resulting from the access and exfiltration, theft, or disclosure of their personal information;

ix. Whether Plaintiff and Class Members are entitled to credit monitoring and other monetary relief;

x. Whether DEFENDANT'S failure to implement and maintain reasonable security procedures and practices constitutes negligence;

xi. Whether DEFENDANT'S failure to implement and maintain reasonable security procedures and practices constitutes negligence per se;

xii. Whether DEFENDANT'S failure to implement and maintain reasonable security procedures and practices constitutes violation of the Federal Trade Commission Act, 15 U.S.C. § 45(a);

xiii. Whether DEFENDANT'S failure to implement and maintain reasonable security procedures and practices constitutes violation of the California Consumer Privacy Act, Cal. Civ.

Code § 1798.150, California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200; and

xiv. Whether the California subclass is entitled to actual pecuniary damages under the private rights of action in the California Customer Records Act, Cal. Civ. Code § 1798.84 and the California Consumer Privacy Act, Civ. Code § 1798.150, and the proper measure of such damages, and/or statutory damages pursuant § 1798.150(a)(1)(A) and the proper measure of such damages.

c. Typicality. The claims of the named Plaintiff are typical of the claims of the Class Members because all had their personal information compromised as a result of DEFENDANT'S failure to implement and maintain reasonable security measures and the consequent data breach.

d. Adequacy of Representation. Plaintiff will fairly and adequately represent the interests of the class. Counsel who represent Plaintiff are experienced and competent in consumer and employment class actions, as well as various other types of complex and class litigation.

e. Superiority and Manageability. A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual joinder of all Plaintiffs is not practicable, and questions of law and fact common to Plaintiffs predominate over any questions affecting only Plaintiff. Each Plaintiff has been damaged and is entitled to recovery by reason of DEFENDANT'S unlawful failure to adequately safeguard their data. Class action treatment will allow those similarly situated persons to litigate their claims in the manner that is most efficient and economical for the parties and the judicial system. As any civil penalty awarded to any individual class member may be small, the expense and burden of individual litigation

make it impracticable for most Class Members to seek redress individually. It is also unlikely that any individual consumer would bring an action solely on behalf of himself or herself pursuant to the theories asserted herein. Additionally, the proper measure of civil penalties for each wrongful act will be answered in a consistent and uniform manner. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action, as DEFENDANT'S records will readily enable the Court and parties to ascertain affected companies and their employees.

f. Notice to Class. Among other means, potential notice to Class Members of this class action can be accomplished via United States mail to all individuals who received a copy of the three Data Breach notice letters and/or through electronic mail and/or through publication.

63. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because DEFENDANT has acted or refused to act on grounds generally applicable to the class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the class as a whole.

64. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of the matters and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether DEFENDANT owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, processing, using, and safeguarding their personal information;

b. Whether DEFENDANT breached that legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, processing, using, and safeguarding their personal information;

c. Whether DEFENDANT failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether DEFENDANT failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information compromised in the breach; and

e. Whether Class Members are entitled to actual damages, credit monitoring, injunctive relief, statutory damages, and/or punitive damages as a result of DEFENDANT'S wrongful conduct as alleged herein.

FIRST CAUSE OF ACTION

(Negligence, By Plaintiff and the Nationwide Class Against DEFENDANT)

65. Plaintiff realleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

66. DEFENDANT owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, storing, using, processing, deleting and safeguarding their personal information in its possession from being compromised, stolen, accessed, and/or misused by unauthorized persons. That duty includes a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information that were compliant with and/or better than industry-standard practices. DEFENDANT'S duties included a duty to design, maintain, and test its security systems to ensure that Plaintiff's and Class Members' personal information was adequately secured and protected, to implement processes that would detect a breach of its security system in a timely manner, to timely act upon warnings and alerts, including those generated by its own security systems

regarding intrusions to its networks, and to promptly, properly, and fully notify its clients, Plaintiff, and Class Members of any data breach.

67. DEFENDANT'S duties to use reasonable care arose from several sources, including but not limited to those described below.

68. DEFENDANT had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their personal information because hackers routinely attempt to steal such information and use it for nefarious purposes, but DEFENDANT also knew that it was more likely than not Plaintiff and other Class Members would be harmed.

69. DEFENDANT'S duty also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as DEFENDANT.

70. Various FTC publications and data security breach orders further form the basis of DEFENDANT'S duty. According to the FTC, the need for data security should be factored into all business decision making.[17] In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[18] Among other things, the guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on

[17] *Start with Security, A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[18] *Protecting Personal Information, A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures. The FBI has also issued guidance on best practices with respect to data security that also form the basis of DEFENDANT'S duty of care, as described above.[19]

71. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' personal information, DEFENDANT assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' personal information from disclosure.

72. DEFENDANT also had a duty to safeguard the personal information of Plaintiffs and Class Members and to promptly notify them of a breach because of state laws and statutes that require DEFENDANT to reasonably safeguard personal information, as detailed herein, including Cal. Civ. Code § 1798.80 *et seq.*

73. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or lock their credit profiles, cancel or change usernames or passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, develop alternative

[19] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last viewed February 3, 2023).

timekeeping methods or other tacks to avoid untimely or inaccurate wage payments, and take other steps to mitigate or ameliorate the damages caused by DEFENDANT'S misconduct.

74. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their personal information.

75. DEFENDANT breached the duties it owed to Plaintiff and Class Members described above and thus was negligent. DEFENDANT breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the personal information of Plaintiff and Class Members; (b) prevent the breach; (c) timely detect the breach; (d) maintain security systems consistent with industry; (e) timely disclose that Plaintiff's and Class Members' personal information in DEFENDANT'S possession had been or was reasonably believed to have been stolen or compromised; (f) failing to comply fully even with its own purported security practices.

76. DEFENDANT knew or should have known of the risks of collecting and storing personal information and the importance of maintaining secure systems, especially in light of the increasing frequency of ransomware attacks. The sheer scope of DEFENDANT'S operations further shows that DEFENDANT knew or should have known of the risks and possible harm that could result from its failure to implement and maintain reasonable security measures. On information and belief, this is but one of the several vulnerabilities that plagued DEFENDANT'S systems and led to the data breach.

77. Through DEFENDANT'S acts and omissions described in this complaint, including DEFENDANT'S failure to provide adequate security and its failure to protect the personal information of Plaintiff and Class Members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, DEFENDANT unlawfully breached their duty to use reasonable care to

adequately protect and secure Plaintiff's and Class Members' personal information.

78. DEFENDANT further failed to timely and accurately disclose to clients, Plaintiff, and Class Members that their personal information had been improperly acquired or accessed and/or was available for sale to criminals on the dark web.

79. But for DEFENDANT'S wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their personal information would not have been compromised.

80. Plaintiff and Class Members relied on DEFENDANT to keep their personal information confidential and securely maintained, and to use this information for business purposes only, and to make only authorized disclosures of this information.

81. As a direct and proximate result of DEFENDANT'S negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. As a result of DEFENDANT'S failure to protect Plaintiff's and Class Members' personal information, Plaintiff's and Class Members' personal information has been accessed by malicious cybercriminals. Plaintiff's and the Class Members' injuries include:

a. theft of their personal information;

b. costs associated with requested credit freezes;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were

permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information being placed in the hands of criminals;

i. damages to and diminution of value of their personal information entrusted, directly or indirectly, to DEFENDANT with the mutual understanding that DEFENDANT would safeguard Plaintiff's and the Class Members' data against theft and not allow access and misuse of their data by others;

j. continued risk of exposure to hackers and thieves of their personal information, which remains in DEFENDANT'S possession and is subject to further breaches so long as DEFENDANT fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members, along with damages stemming from the stress, fear, and anxiety of an increased risk of identity theft and fraud stemming from the breach;

k. loss of the inherent value of their personal information;

l. the loss of the opportunity to determine for themselves how their personal information is used; and

m. other significant additional risk of identity theft, financial fraud, and other identity-related fraud in the indefinite future.

82. In connection with the conduct descried above, DEFENDANT acted wantonly, recklessly, and with complete disregard for the consequences Plaintiff and Class Members would suffer if their highly sensitive and confidential personal information, including but not limited to name, company name, address, social security numbers, and banking and credit card information, was access by unauthorized third parties.

SECOND CAUSE OF ACTION
(Negligence Per Se, By Plaintiff and the Nationwide Class Against DEFENDANT)

83. Plaintiff realleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

84. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as DEFENDANT. Various FTC publications and data security breach orders further form the basis of DEFENDANT'S duty. In addition, individual states have enacted statutes based on the FTC Act that also created a duty.

85. DEFENDANT violated Section 5 of the FTC Act by failing to use reasonable measures to protect personal information and not complying with industry standards. DEFENDANT'S conduct was particularly unreasonable given the nature and amount of personal information it obtained and stored and the foreseeable consequences of a data breach.

86. DEFENDANT'S violation of Section 5 of the FTC Act constitutes

negligence *per se*.

87. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was meant to protect.

88. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the Class.

89. As a direct and proximate result of DEFENDANT'S negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
(Declaratory Judgment, By Plaintiff and the Nationwide Class Against DEFENDANT)

90. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

91. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this complaint.

92. An actual controversy has arisen in the wake of the DEFENDANT'S data breach regarding its present and prospective common law and other duties to reasonably safeguard consumers personal identifying information in its possession, custody and/or control and regarding whether DEFENDANT is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their personal information. Plaintiff alleges that DEFENDANT'S data security measures remain inadequate.

DEFENDANT denies these allegations. Plaintiff continues to suffer injury as a result of the compromise of his personal information and remains at imminent risk that further compromises of her personal information will occur in the future.

93. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. DEFENDANT continues to owe a legal duty to secure consumers' personal information, including Plaintiff's and Class Members' personal information, to timely notify them of a data breach under the common law, Section 5 of the FTC Act; and

b. DEFENDANT continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff's and Class Members' personal information.

94. The Court should issue corresponding prospective injunctive relief requiring DEFENDANT to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and Class Members' personal information.

95. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at DEFENDANT. The risk of another such breach is real, immediate, and substantial. If another breach at DEFENDANT's occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

96. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to DEFENDANT if an injunction is issued. Among other things, if another massive data breach occurs, Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to DEFENDANT of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and DEFENDANT has a

pre-existing legal obligation to employ such measures.

97. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Plaintiff and the thousands of Class Members whose confidential information would be further compromised.

FOURTH CAUSE OF ACTION
(Violation of the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq.*, § 1798.150(a) By Plaintiff and the California Subclass Against DEFENDANT)

98. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

99. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> > (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
> >
> > (B) Injunctive or declaratory relief.
> >
> > (C) Any other relief the court deems proper.

100. DEFENDANT is a "business" under § 1798.140(b) in that it is a

corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million.

101. Plaintiff and California Subclass Members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

102. The personal information of Plaintiff and the California Subclass at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information DEFENDANT collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

103. DEFENDANT knew or should have known that its computer systems and data security practices were inadequate to safeguard the California Subclass's personal information and that the risk of a data breach or theft was highly likely. DEFENDANT failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass. Specifically, DEFENDANT subjected Plaintiff's and the California Subclass's nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure

as a result of the DEFENDANT'S violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

104. As a direct and proximate result of DEFENDANT'S violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiff and Class Members' personal information included exfiltration, theft, or disclosure through DEFENDANT'S servers, systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

105. As a direct and proximate result of DEFENDANT'S acts, Plaintiff and the California Subclass were injured and lost money or property, including but not limited to the loss of Plaintiff's and the subclass's legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

106. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages." Accordingly, Plaintiff and the California Subclass by way of this complaint seek actual pecuniary damages suffered as a result of DEFENDANT'S violations described herein. Plaintiff will issue a notice of these alleged violations pursuant to § 1798.150(b) forthwith. After the expiration of the period to cure the defects alleged, Plaintiff intends to amend this complaint to seek statutory damages and injunctive relief pursuant to §1798(a)(1)(A)-(C), (a)(2), and (b).

FIFTH CAUSE OF ACTION

(Violation of the California Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*,
By Plaintiff and the California Subclass Against DEFENDANT)

107. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

108. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

109. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

110. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

111. Plaintiff and members of the California Subclass are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to DEFENDANT, directly and/or indirectly, for the purpose of obtaining a service from DEFENDANT.

112. The personal information of Plaintiff and the California Subclass at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information DEFENDANT collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or

debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

113. DEFENDANT knew or should have known that its computer systems and data security practices were inadequate to safeguard the California Subclass's personal information and that the risk of a data breach or theft was highly likely. DEFENDANT failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass. Specifically, DEFENDANT failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and the California Subclass from unauthorized access, destruction, use, modification, or disclosure. DEFENDANT further subjected Plaintiff's and the California Subclass's nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the DEFENDANT'S violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

114. As a direct and proximate result of DEFENDANT'S violation of their duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiff and the California Subclass included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and the California Subclass by the ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

115. As a direct and proximate result of DEFENDANT'S acts or omissions,

Plaintiff and the California Subclass were injured and lost money or property including, but not limited to, the loss of Plaintiff's and the Subclass's legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

116. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

117. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;
b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
c. If the information is possible to determine at the time the notice is provided, then any of the following:
    i. the date of the breach,
    ii. the estimated date of the breach, or
    iii. the date range within which the breach occurred. The notification shall also include the date of the notice;
d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

118. DEFENDANT failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the California Subclass. On information and belief, to date, DEFENDANT has not sent written notice of the data breach to all impacted individuals. As a result, DEFENDANT has violated § 1798.82 by not providing legally compliant and timely notice to all Class Members. Because not all members of the class have been notified of the breach, members could have taken action to protect their personal information, but were unable to do so because they were not timely notified of the breach.

119. On information and belief, many Class Members affected by the breach have not received any notice at all from DEFENDANT in violation of Section 1798.82(d).

120. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

121. As a direct consequence of the actions as identified above, Plaintiff and Class Members incurred additional losses and suffered further harm to their

privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

SIXTH CAUSE OF ACTION

(Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §17200 *et seq.*
By Plaintiff and the California Subclass Against DEFENDANT)

122. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

123. DEFENDANT is a "person" defined by Cal. Bus. & Prof. Code § 17201.

124. DEFENDANT violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

125. DEFENDANT'S "unfair" acts and practices include:

a. DEFENDANT failed to implement and maintain reasonable security measures to protect Plaintiff's and California Subclass Members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the DEFENDANT'S data breach. DEFENDANT failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. DEFENDANT'S failure to implement and maintain reasonable

security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. DEFENDANT'S failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of DEFENDANT'S inadequate security, consumers could not have reasonably avoided the harms that DEFENDANT caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

126. DEFENDANT has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law.

127. DEFENDANT'S unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass Members' personal information, which was a direct and proximate cause of the DEFENDANT'S data breach;

b. Failing to identify foreseeable security and privacy risks, remediate

identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the DEFENDANT'S data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, which was a direct and proximate cause of the DEFENDANT'S data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass Members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass Members' personal information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' personal information, including duties imposed by the FTC Act, 15

U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150.

128. DEFENDANT'S representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of DEFENDANT'S data security and ability to protect the confidentiality of consumers' personal information.

129. As a direct and proximate result of DEFENDANT'S unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass Members' were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

130. DEFENDANT'S violations were, and are, willful, deceptive, unfair, and unconscionable.

131. Plaintiff and Class Members have lost money and property as a result of DEFENDANT'S conduct in violation of the UCL, as stated herein and above.

132. By deceptively storing, collecting, and disclosing their personal information, DEFENDANT has taken money or property form Plaintiff and Class Members.

133. DEFENDANT acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California Subclass members' rights. Past data breaches put it on notice that its security and privacy protections were inadequate.

134. Plaintiff and California Subclass Members' seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from DEFENDANT'S unfair, unlawful, and fraudulent business practices or use of

their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

SEVENTH CAUSE OF ACTION
(Invasion of Privacy)
(Count 1 – Common Law Invasion of Privacy – Intrusion Upon Seclusion By Plaintiff and the Nationwide Class Against DEFENDANT)

135. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

136. To assert claims for intrusion upon seclusion, one must plead (1) that the defendant intentionally intruded into a matter as to which plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

137. DEFENDANT intentionally intruded upon the solitude, seclusion and private affairs of Plaintiff and Class Members by intentionally configuring their systems in such a way that left them vulnerable to malware/ransomware attack, thus permitting unauthorized access to their systems, which compromised Plaintiff's and Class Members' personal information. Only DEFENDANT had control over its systems.

138. DEFENDANT'S conduct is especially egregious and offensive as they failed to have adequate security measures in place to prevent, track, or detect in a timely fashion unauthorized access to Plaintiff's and Class Members' personal information.

139. At all times, DEFENDANT was aware that Plaintiff's and Class Members' personal information in their possession contained highly sensitive and confidential personal information.

140. Plaintiff and Class Members have a reasonable expectation of privacy in their personal information, which also contains highly sensitive medical

information.

141. DEFENDANT intentionally configured their systems in such a way that stored Plaintiff's and Class Members' personal information to be left vulnerable to malware/ransomware attack without regard for Plaintiff's and Class Members' privacy interests.

142. The disclosure of the sensitive and confidential personal information of thousands of consumers, was highly offensive to Plaintiff and Class Members because it violated expectations of privacy that have been established by general social norms, including by granting access to information and data that is private and would not otherwise be disclosed.

143. DEFENDANT'S conduct would be highly offensive to a reasonable person in that it violated statutory and regulatory protections designed to protect highly sensitive information, in addition to social norms. DEFENDANT'S conduct would be especially egregious to a reasonable person as DEFENDANT publicly disclosed Plaintiff's and Class Members' sensitive and confidential personal information without their consent, to an "unauthorized person," i.e., hackers.

144. As a result of DEFENDANT'S actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

145. Plaintiff and Class Members have been damaged as a direct and proximate result of DEFENDANT'S intrusion upon seclusion and are entitled to just compensation.

146. Plaintiff and Class Members are entitled to appropriate relief, including compensatory damages for the harm to their privacy, loss of valuable rights and protections, and heightened stress, fear, anxiety and risk of future invasions of privacy.

(Count 2 –Invasion of Privacy – Cal. Const. Art. 1, § 1
By Plaintiff and the California Subclass Against DEFENDANT)

147. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

148. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

149. The right to privacy in California's constitution creates a private right of action against private and government entities.

150. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

151. DEFENDANT violated Plaintiff's and Class Members' constitutional right to privacy by collecting, storing, and disclosing their personal information in which they had a legally protected privacy interest, and in which they had a reasonable expectation of privacy in, in a manner that was highly offensive to Plaintiff and Class Members, would be highly offensive to a reasonable person, and was an egregious violation of social norms.

152. DEFENDANT has intruded upon Plaintiff's and Class Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential personal information.

153. DEFENDANT'S actions constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the invasion occurred within a zone of privacy protected by the California Constitution, namely the misuse of information gathered for an improper purpose; and (ii) the invasion deprived Plaintiff and Class Members of the ability to control the circulation of their personal information, which is considered fundamental to the right to privacy.

154. Plaintiff and Class Members had a reasonable expectation of privacy in that: (i) DEFENDANT'S invasion of privacy occurred as a result of DEFENDANT'S security practices including the collecting, storage, and unauthorized disclosure of consumers' personal information; (ii) Plaintiff and Class Members did not consent or otherwise authorize DEFENDANT to disclosure their personal information; and (iii) Plaintiff and Class Members could not reasonably expect DEFENDANT would commit acts in violation of laws protecting privacy.

155. As a result of DEFENDANT'S actions, Plaintiff and Class Members have been damaged as a direct and proximate result of DEFENDANT'S invasion of their privacy and are entitled to just compensation.

156. Plaintiff and Class Members suffered actual and concrete injury as a result of DEFENDANT'S violations of their privacy interests. Plaintiff and Class Members are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by DEFENDANT'S invasions.

157. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as well as disgorgement of profits made by DEFENDANT as a result of its intrusions upon Plaintiff's and Class Members' privacy.

EIGHTH CAUSE OF ACTION
(Breach of Implied Contract)
(By Plaintiff and the Nationwide Class Against DEFENDANT)

170. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

171. Through its course of conduct, DEFENDANT, Plaintiff and Class Members entered into implied contracts for DEFENDANT to implement data

security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

172. DEFENDANT required Plaintiff and Class Members to provide and entrust their PII as a condition of obtaining DEFENDANT'S services.

173. DEFENDANT solicited and invited Plaintiff and Class Members to provide their PII as part of DEFENDANT'S regular business practices. Plaintiff and Class Members accepted DEFENDANT'S offers and provided their PII to DEFENDANT.

174. Plaintiff and Class Members provided and entrusted their PII to DEFENDANT. In so doing, Plaintiff and Class Members entered into implied contracts with DEFENDANT by which DEFENDANT agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if its data had been breached and compromised or stolen.

175. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to DEFENDANT, in exchange for, amongst other things, the protection of their PII.

176. Plaintiff and Class Members fully performed their obligations under the implied contracts with DEFENDANT.

177. DEFENDANT breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

178. As a direct and proximate result of DEFENDANT'S above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic

harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

NINTH CAUSE OF ACTION
(Breach of the Implied Covenant of Good Faith and Fair Dealing)
(By Plaintiff and the Nationwide Class Against DEFENDANT)

179. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

180. Every contract in this state has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

181. Plaintiff and Class Members have complied with and performed all conditions of their contracts with DEFENDANT.

182. DEFENDANT breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and storage of other personal information after DEFENDANT knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach. DEFENDANT acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself, the nationwide class and the California subclass pray for the following relief:

1. An order certifying the nationwide Class and California Subclass as defined above pursuant to Fed. R. Civ. P. 23 and declaring that Plaintiff is proper class representative and appointing Plaintiff's counsel as class

counsel;

2. Permanent injunctive relief to prohibit DEFENDANT from continuing to engage in the unlawful acts, omissions, and practices described herein;
3. Compensatory, consequential, general, and nominal damages in an amount to be proven at trial, in excess of $5,000,000;
4. Disgorgement and restitution of all earnings, profits, compensation, and benefits received as a result of the unlawful acts, omissions, and practices described herein;
5. Punitive, exemplary, and/or trebled damages to the extent permitted by law;
6. Plaintiff intends to amend this complaint to seek statutory damages on behalf of the California subclass upon expiration of the 30-day cure period pursuant to Cal. Civ. Code § 1798.150(b);
7. A declaration of right and liabilities of the parties;
8. Costs of suit;
9. Reasonable attorneys' fees, including pursuant to Cal. Civ. Pro. Code § 1021.5;
10. Pre- and post-judgment interest at the maximum legal rate;
11. Distribution of any monies recovered on behalf of members of the class or the general public via fluid recovery or *cy pres* recovery where necessary and as applicable to prevent Defendant from retaining the benefits of their wrongful conduct; and
12. Such other relief as the Court deems just and proper.

Dated: June 7, 2024

WUCETICH & KOROVILAS LLP

By: /s/ Jason M. Wucetich
JASON M. WUCETICH
Attorneys for Plaintiff ANTONIO HOOD, individually and on behalf of all others similarly situated

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the putative class and subclass, hereby demand a trial by jury on all issues of fact or law so triable.

Dated: June 7, 2024

WUCETICH & KOROVILAS LLP

By: /s/ Jason M. Wucetich
JASON M. WUCETICH
Attorneys for Plaintiff ANTONIO HOOD, individually and on behalf of all others similarly situated